1. (Currently Amended) A method of affecting a trustworthy-measure associated with a source node in a distributed network, the method comprising:

receiving an information file from the source node and a corresponding identifying code that is based on content of the information file when the information file is introduced to the network, and computing an associated code based on received content of the information file;

comparing the associated code with the identifying code; ~~and~~

transmitting an error report to an administrator node, the error report identifying the source node and the information file, when at least one of the following occur: the associated code does not correspond to the identifying code, and the content of the information file is abnormal; and

reducing the value of ~~thereby facilitating a reduction of~~ the trustworthy-measure associated with the source node in response to the error report, thereby providing the reduced-value trustworthy measure for evaluating subsequent use of the source node.

2. (Currently Amended) The method of claim 1,

wherein transmitting an error report includes transmitting an error report in response to the step of comparing indicating that a difference between the associated code and the identifying code is not caused by a communication error, and

further including: repeating the receiving, computing, and comparing steps prior to transmitting the error report.

3. (Previously presented) The method of claim 1, wherein the identifying code includes at least one of: a control-sum-code, and a hash-value.

4. (Previously presented) The method of claim 1, wherein the error report includes the associated code and the identifying code.

5. (Currently Amended) A method of facilitating control of distribution of modified or corrupted files in a distributed network, the method comprising:

providing a catalog of available files to nodes of the distributed network, the catalog identifying each file of the available files and a corresponding source node of each file,

processing an error report from a target node that received a downloaded file from a selected source node,

verifying the error report,

degrading a trustworthy-measure of at least one node of the distributed network based on a result of verifying the error report, and

providing the trustworthy-measure of the at least one node to other nodes of the distributed network.

6. (Currently Amended) The method of claim 5, wherein

degrading a trustworthy-measure includes degrading a trustworthy-measure of a node to a non-zero value that is less than a previous value of the trustworthy-measure of the node, and

the catalog includes a parameter that is based on the trustworthy-measure of each source node.

7. (Previously presented) The method of claim 5, wherein the error report is based on at least one of: a modification of an original version of the downloaded file, and an abnormality associated with the downloaded file.

8. (Previously presented) The method of claim 5, wherein verifying the error report is based upon an identifying code corresponding to an original version of the downloaded file.

9. (Previously presented) The method of claim 8, wherein the catalog includes the identifying code.

10. (Currently Amended) A method of controlling a trustworthy-measure associated with a source node in a distributed network, the method comprising:

receiving, from a reporting node, a report of a modification or corruption of an information file by the source node,

determining a validity of the report, and

degrading the trustworthy-measure associated with the source node when the report is determined to be valid.

11. (Previously presented) The method of claim 10, wherein determining the validity of the report includes: receiving, from the source node, the information file and a corresponding identifying code that is based on content of the information file when the information file is introduced to the network, computing a verification code based on received content of the information file, comparing the verification code with the identifying code.

12. (Previously presented) The method of claim 10, further including degrading a trustworthy-measure associated with the reporting node when the report is determined to be invalid.

13. (Previously presented) The method of claim 10, further including allowing the trustworthy-measure to be accessed by other nodes in the distributed network, to influence subsequent requests for material from the source node, based on the trustworthy-measure.

14. (Previously presented) The method of claim 10, wherein determining the validity of the report includes notifying the source node of the report, and assessing a response from the source node to determine the validity of the report.

15. (Previously presented) The method of claim 14, wherein

receiving a report of a modification or corruption of an information file by the source node includes receiving a report that the modification or corruption was not caused by a communication error, and assessing the response includes: determining that the report is valid if the response is a null-response, or an admittance of effecting the modification or corruption of the information, and revising the report to identify an alternative source of the modification or corruption of the information, if the response includes an acknowledgement of the modification or corruption.

16. (Previously presented) The method of claim 14, wherein assessing the response includes assessing the reliability of at least one of: the information file, the source node, and the reporting node.

17. (Previously presented) The method of claim 10, wherein determining the validity of the report includes determining a reliability of the source node, and determining the reliability of the source node is based on at least one of the trustworthy-measure of the source node, longevity of the source node within the distributed network, traffic flow via the source node, and prior activities of the source node.

18. (Previously presented) The method of claim 17, wherein determining the validity of the report also includes determining a reliability of the reporting node, and determining the reliability of the reporting node is based on at least one of: the trustworthy-measure of the reporting node, longevity of the reporting node within the distributed network, traffic flow via the reporting node, and prior activities of the reporting node.

19. (Previously presented) The method of claim 10, wherein determining the validity of the report includes a verification of prior ownership of the information file.

20. (Currently Amended) A communications network, comprising:

a plurality of nodes, including at least a source node, a target node, and an administrator node, the source node having an information file and a corresponding identifying code based on content of the information file at a prior point in time,

the target node being configured to: receive the information file and identifying code, transmit a discrepancy report based on at least one of: a discrepancy between the identifying code and a computed code based on received content of the information file, and an abnormality in the information file, and

the administrator node being configured to: receive the discrepancy report, and modify a trustworthy-measure associated with at least one node of the plurality of nodes, based on the discrepancy report.

21. (Currently Amended) The communications network of claim 20, wherein the administrator node is further configured to verify the discrepancy report prior to modifying the trustworthy-measure by verifying that the discrepancy report is indicative of a modification or corruption of an information file by the source node that is not based upon a communication error.

22. (Previously presented) The communications network of claim 21, wherein the administrator node is configured to verify the discrepancy report by: receiving the information file from the source node, and determining a verification code based on received content of the information file, and comparing the verification code to the identifying code.

23. (Previously presented) The communications network of claim 21, wherein the administrator node is configured to verify the discrepancy report based on at least one of: a reliability of the received content of the information file, a record of prior ownership of the information file, a reliability of the source node, a reliability of the reporting node, a longevity of the source node within the network, a longevity of the reporting node within the network, prior activities of the source node within the network, and prior activities of the reporting node within the network.

24. (Previously presented) The communications network of claim 23, wherein the trustworthy-measure of the source node is available for access by each of the plurality of nodes, to facilitate control of subsequent distribution of files from the source node based on the trustworthy-measure.

25. (Previously presented) An administrator node in a distributed communications network for exchanging information files among a plurality of nodes, the administrator node configured to: receive a discrepancy report from a reporting node, the discrepancy report identifying a source node and an information file, verify the discrepancy report, and modify a trustworthy-measure associated at least one node of the plurality of nodes, based on whether the discrepancy report is valid.

26. (Currently Amended) The administrator node of claim 25, wherein the discrepancy report is based on a comparison of a code computed by the reporting node to an identifying code corresponding to contents of the information file at a prior time to determine that the discrepancy report identifies a discrepancy that is not due to a communication error, the administrator node is configured to verify the discrepancy report by: receiving the information file from the source node, and determining a verification code based on received content of the information file, and comparing the verification code to the identifying code

27. (Previously presented) The administrator node of claim 25, wherein the administrator node is configured to verify the discrepancy report based on at least one of a reliability of the received content of the information file, a record of prior ownership of the information file, a reliability of the source node, a reliability of the reporting node, a longevity of the source node within the network, a longevity of the reporting node within the network, prior activities of the source node within the network, and prior activities of the reporting node within the network.

28. (Previously presented) The administrator node of claim 25, wherein the administrator node is further configured to provide a catalog that identifies a plurality of information files and corresponding source nodes.

29. (Previously presented) The administrator node of claim 28, wherein the catalog further includes a parameter based on the trustworthy-measure of the at least one node.

30. (Previously presented) The method of claim 2, wherein repeating the receiving, computing, and comparing steps prior to transmitting the error report is used to determine whether information file errors were caused during or prior to communication of the information file from the source node.

31. (Previously presented) The method of claim 30, further comprising preventing transmitting the error report upon determining that the information file errors were caused during communication.

32. (Previously presented) The method of claim 5, wherein verifying the error report includes determining an originator node responsible for modifications to the downloaded file giving rise to the error report.

33. (Previously presented) The method of claim 32, wherein determining the originator node includes notifying the selected source node, and assessing a response from the selected source node to determine the validity of the error report.

34. (Previously presented) The method of claim 33, wherein assessing the response includes determining that the error report is valid if the response is a null-response or an admittance of causing the modifications to the downloaded file, and revising the report to identify an alternative source of the modifications to the downloaded file if the response includes an acknowledgement of the modifications.